お知らせ

2024 年 9 月 11 日
SCSK株式会社

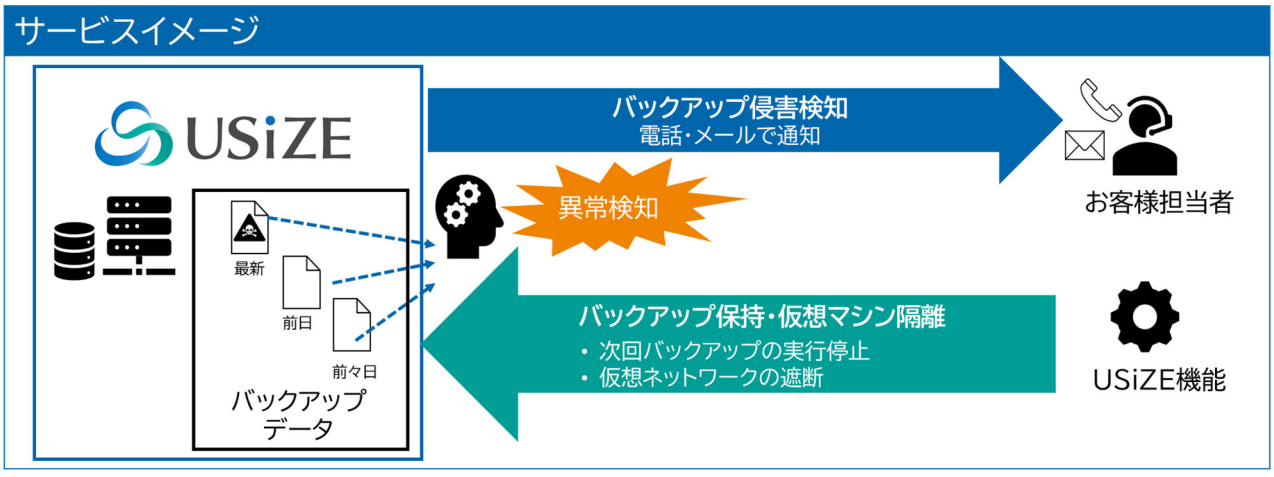
「USiZE」のランサムウェア対応サービスに新サービスを追加
～バックアップデータ内のランサムウェアによる被害を検知し、初動対応を自動化～

SCSK株式会社（本社：東京都江東区、代表取締役　執行役員　社長：當麻　隆昭、以下　SCSK）は、プライベートクラウドサービス「USiZE（ユーサイズ）」において、Rubrik Japan 株式会社（以下　Rubrik 社）が提供する「Rubrik Security Cloud」と連携した「ランサムウェア対応サービス」※に「バックアップ保持・仮想マシン隔離」（以下　本サービス）を新たに追加し、2024 年 9 月 11 日より提供を開始します。
2024 年 5 月に発表した「ランサムウェア対応サービス　バックアップ侵害検知」に続く本サービスは、ランサムウェア攻撃を受けた際の初動対応を自動化することで、迅速な対応を可能にします。
※「ランサムウェア対応サービス　バックアップ侵害検知」について：https://www.scsk.jp/news/2024/pdf/20240521.pdf

1. サービスの概要と特長

本サービスは、Rubrik 社が提供する「Rubrik Security Cloud」の機能を活用し、バックアップデータを分析して、ランサムウェアによる攻撃の疑いを検出します。攻撃が疑われる仮想マシンに対して、自動で次回以降のバックアップ実行停止、仮想ネットワークの遮断を行います。これにより、手動対応と比べて対応時間と運用負荷を大幅に削減することが可能です。これらの初動対応は仮想マシンの台数が多いほど時間がかかるため、多くの仮想マシンを利用中のお客様ほど効果的です。

- **機械学習による検出**：機械学習を使用してランサムウェア攻撃によって生じるデータに対して異常な挙動や変更を検出します。
- **自動化された初動対応**：ランサムウェア攻撃を受けた際の初動対応を自動で実行し、迅速な対応を実現します。
- **バックアップデータの保護**：次回バックアップの実行停止により、システム復旧に不可欠な攻撃を受けていないバックアップデータが削除されることを防ぎます。また復旧に使用できない攻撃を受けたデータのバックアップ取得を防ぐことで、使用可能か調査する対象を減らし特定までにかかる時間を削減することが可能です。
- **感染拡大の防止**：仮想ネットワークの遮断により、他の仮想マシンへの感染拡大を防ぎます。



2. 提供価格

仮想マシンの利用台数等にかかわらず、一律月額　50,000 円

3. 今後の展望

被害範囲の特定までにかかる時間を削減する変更、暗号化されたファイルの特定や復旧に利用可能なバックアップデータをテストする隔離環境の提供など、データ復旧の支援のために Rubrik 社のソリューションを活用したサービスの拡充を図ります。

本件に関するお問い合わせ先

SCSK株式会社
ソリューション事業グループ
クラウドサービス事業本部　USiZE サービス部
E-mail：usize-info@scsk.jp